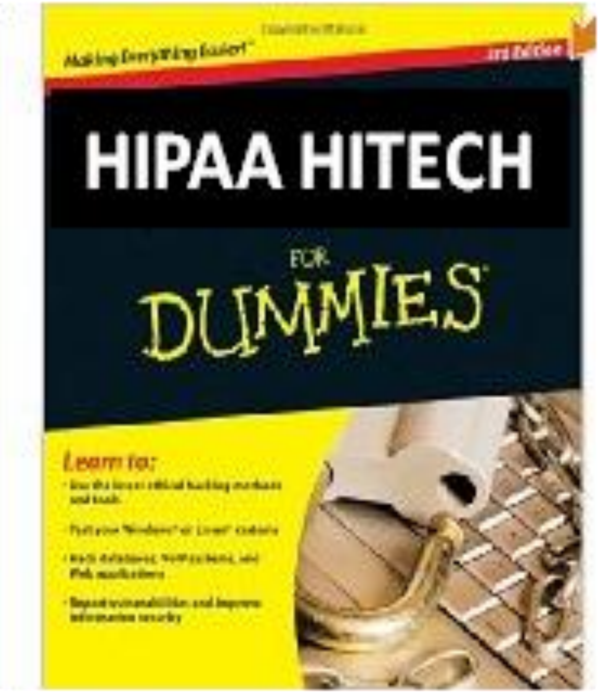
the industry radar
Business Network

The Industry Radar Business Network

Presents



Protecting Your Clients and Your Business:

From Risk Assessment to Compliance and Encryption

3.1.2010

Disclaimer: This document and its references do not constitute legal advice. Consult qualified counsel for any legal issues that concern you, your organization, or questions of compliance

the industry radar
Business Network

What Business Associates (BA's) Must Do To Be HIPAA HITECH Compliant

What is HITECH: The Health Information Technology for Economic and Clinical Health Act (HITECH) significantly expanded the reach of the HIPAA Privacy Rule and Security Rule, along with the corresponding penalties.

> *"While you have always been contractually obligated to abide by HIPAA this new law now requires that you be legally compliant as well."*
> **Assurant BA Agreement**

What does HITECH Do?

- HIPAA now applies to HIPAA to covered entities (CE) business associates (BAs) directly.
- HITECH includes a statutory obligation for BAs to comply with HIPAA.
- HITECH also requires PHI breach notification, which was not part of the original HIPAA rules.
- HITECH also substantially increased the penalties for HIPAA violations

Why HITECH Applies to You – Brokers/agents are BA's if they have BA agreements with any insurer ***and/or*** receive, create, transmit or maintain personal health information (PHI). Census, enrollment, claims info et al are PHI.

> **PHI** - *"any information, whether oral or recorded in any form or medium, …created or received by a health care provider, health plan, employer, life insurer, …health care clearinghouse… for the past, present, or future payment for the provision of health care to an individual… including demographic information collected from an individual… that identifies the individual; or …with respect to which there is a reasonable basis to believe the information can be used to identify the individual."*

Compliance Overview - A broad overview (detailed plans follow on pgs 2-4) of work that needs to be done by all BA's, regardless of size:

- Appoint a chief privacy/security officer
- Do a full risk assessment of you business, get a gap analysis and focus on those areas to fix
- Privacy and Security Policies Documented and in place
- Implement all HIPAA security administrative, technical and physical safeguards
- Get encryption in place for all PHI your organization handles and communicates
- Update/establish business associate agreements with your clients and vendors
- Conduct privacy and security workforce training
- Comply with new notification rules for breach of unsecured PHI

New Breach Rules - HITECH establishes mandatory federal breach reporting requirements for HIPAA CE's and their BA's, as well as a new "Tattle" rule which requires BA's to report their CE's breaches. It also requires local media notification as mandatory if a breach involves 500 or more lives in one state.

New Enforcement and Penalties - State Attorneys General to can now take legal action on HIPAA privacy/security violations. CT took the first action against Health Net last month. BAs that violate the security and privacy provisions of HIPAA are subject to the same new and beefed up civil and criminal penalties as a covered entity:

Violation	Penalty/Violation	Maximum per Year
Tier A - Did not Know	100	25,000
Tier B - Reasonable cause, not willful neglect	$1,000	100,000
Tier C - "Willful Neglect", corrected	$10,000	$250,000
Tier D - "Willful Neglect", uncorrected	$50,000	$1,500,000

Compliance Deadline – 2/17/2010. Failure to be compliant will likely be viewed as "willful neglect". There is no such thing as partial compliance. It is all or nothing for all CE's and BA's, not just you.

Disclaimer: This document and its references do not constitute legal advice. Consult qualified counsel for any legal issues that concern you, your organization, or questions of compliance

Step I - Risk Assessment and Risk Mitigation:

The first and most important step is to undertake a holistic risk assessment that examines the risks and controls related to four critical areas: processes, people, technology and governance.

In simplest terms the 3 security rules areas that need to be assessed are:

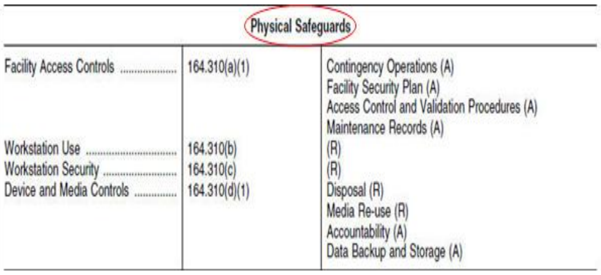
- Administrative - policies, procedures, agreements
- Physical - computers, office et al
- Technical - encryption of communication

When considering the organization's processes, closely examine business and IT processes. For example:

- Determine how PHI is used in ***each business process*** – both paper and electronic.
- When assessing issues related to people, consider the following:
  - Is ***staff trained*** in the secure handling of paper and electronic health records?
  - Do the ***policies and procedures*** provide employees with adequate and up-to-date guidance?
- Next, examine the technology side.
  - Conduct a ***vulnerability assessment*** of the network.
- Pair the vulnerabilities to relevant threats for a complete picture.
  - If encryption is present, is it the most up-to-date encryption algorithm?
  - Is the patch management program operating effectively?
- Inventory and ***review all outsourced service provider agreements***.
  - Request auditor attestations, such as SAS 70 reports, from service providers that process significant transactions.
  - Ensure a "right to audit" clause is defined in the contract.
- Finally, look at ***governance issues***: Identify the individuals who are responsible for the program.
  - In the event of a breach, who will promptly notify management?
  - Who is responsible for making sure timely information security reviews are done?

Physical Safeguards - *(45 C.F.R. § 164.310) must be enacted and monitored:*

- How is PHI stored within the organization (i.e. fixed server databases/hard drives versus removable media such as backup tapes)?
- Does your company have a physical security plan?
- What types of controls exists to limit access into buildings containing servers that host PHI?
- What types of controls exists to limit access within buildings to rooms housing servers containing PHI?



Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

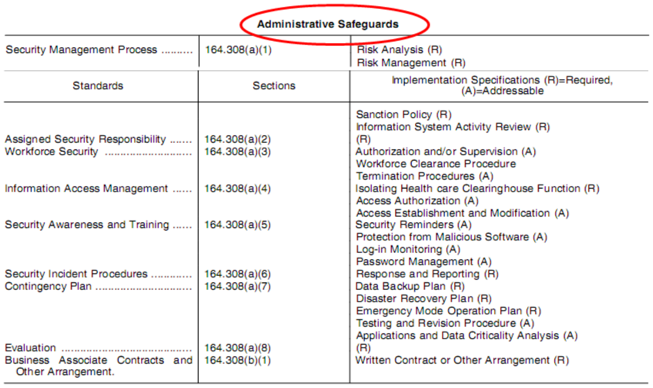
- Who has access to facilities containing PHI, and what process exists to grant these individuals access?
- What environmental controls exist to protect PHI from destruction?
- To the extent PHI is physically maintained, does the organization employ shredders or other destroying devices for confidential PHI containing documents?
  - Do you train and document the training of employees on the use of shredders?

Disclaimer: This document and its references do not constitute legal advice. Consult qualified counsel for any legal issues that concern you, your organization, or questions of compliance

Administrative Safeguards (45 C.F.R. § 164.308): *Policies/Documentation (45 C.F.R. § 164.316)*

What policies (and procedures) are available specifically addressing HIPAA privacy and security rules and compliance including the following:

1. Risk Management
2. Risk Assessment and Application Criticality Analysis (FIPS 200)
3. Physical Security
4. Encryption
5. Remote Access
6. Media and Document Destruction
7. Change Control/ Patch Management
8. Acceptable Use (Email, Portable Media, Software, Company Resources)
9. Training and Security Reminders
10. Antivirus and Workstation Security
11. Unique User Identification
12. Audit and Log Monitoring
13. Security Incident
14. Contingency and Emergency Access and
15. Workforce Clearance, Sanction, and Access Management.



Administrative Safeguards

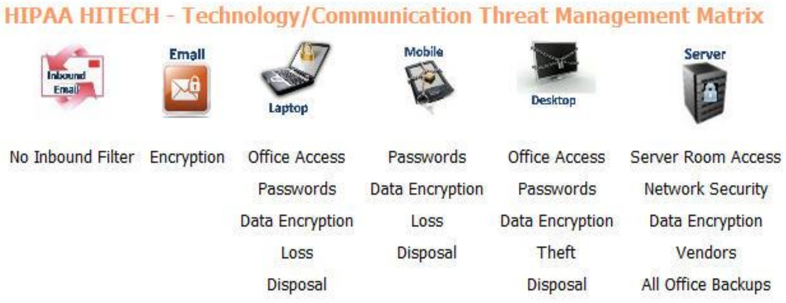
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R)
Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
		Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)

- Who or what group within the organization is responsible for creating and updating these policies?
- When the organization's policies were last updated?
- How often have any of these policies been updated?
- Are new employees trained to follow these policies and procedures?
- How frequently are existing employees re-trained on existing policies and procedures?
- How frequently are existing employees trained regarding updates in HIPAA rules?
- How are personnel screened in order to grant certain levels of access to PHI?
- Does the organization have a formal security incident response plan to address potential breaches of security that include at a minimum:
    1. Roles and responsibilities
    2. Isolate affected system
    3. Preserve evidence
    4. Restore compromised system from known safe backups and
    5. Post incident response report including identification of lessons learned and other mitigating controls may be indicated based on the incident?
- Does the organization require business partners to comply with its privacy and security policies?
- Does organization ever send PHI via email or ftp (file transfer protocol)?
- Does the organization have policy or procedures related to de-identifying PHI for use in advertising, marketing, educational programs?
- What policies and procedures exist regarding notification in the event of a breach?

Disclaimer: This document and its references do not constitute legal advice. Consult qualified counsel for any legal issues that concern you, your organization, or questions of compliance

the industry radar Business Network

Technical Safeguards – (45 C.F.R. § 164.312) are critical and the crux of all your security:



HIPAA HITECH - Technology/Communication Threat Management Matrix

Inbound Email	Email	Laptop	Mobile	Desktop	Server
No Inbound Filter	Encryption	Office Access	Passwords	Office Access	Server Room Access
		Passwords	Data Encryption	Passwords	Network Security
		Data Encryption	Loss	Data Encryption	Data Encryption
		Loss	Disposal	Theft	Vendors
		Disposal		Disposal	All Office Backups

- What types of security exists to protect PHI as it flows to/is accessed at remote workstations?
- Describe the data flow "life-cycle" of PHI through the organization's information systems.
    - This should cover hosting services, TPA, wellness, claims audit, actuarial and other partners including sub agents.
- Does the organization prevent browsers with un-patched security vulnerabilities from accessing the company's information system?
- What types of security and encryption protect portable media containing PHI? (Portable media should always be encrypted.)
    - Equipment Encryption Inventory & Checklist
    - Policy and Audits
        - Regularly verify or audit that encryption policies are in place and being followed.
    - Passwords
        - Use a strong password different than your computer login
        - Never write a password down.
        - Do not share passwords
    - Portable Devices Inventory
        - Know what PHI is stored on all portable devices.
        - Minimize the amount of PHI on portable devices (none in identifiable form).
        - Delete PHI from all portable devices as soon finished working with it.
        - Only use portable storage devices like USB keys, with encryption installed, or install encryption on them before use them to store PHI.
    - PC/Laptop/PDA/Server
        - Enable operating system encryption.
        - Purchase systems with whole disk encryption OR
        - Purchase software for whole disk or virtual disk encryption on laptops/ PDA.
        - Only store PHI on an encrypted disk.
- Does the organization have routine maintenance protocols that backup, delete, relocate, or otherwise impact data containing PHI?
- What types of audit mechanisms exist to track access PHI by internal or external users?
    - Typically audit logs include a timestamp, a unique user account, data accessed/modified/created, and the location of the user.
    - How often are these audit mechanisms used to detect abnormal use?
- Do automatic triggers exist to notify the organization of abnormal PHI use?

Unsecured PHI - Section 13402 of the HITECH Act defined "unsecured" PHI as information that was not secured through the use of technology ***rendering the information "unusable, unreadable or indecipherable.".” i.e encrypted or destroyed.***

Safe Harbor - Use of encryption for PHI is ***a "Safe Harbor"*** under the HITECH law and 47 state privacy laws.

Disclaimer: This document and its references do not constitute legal advice. Consult qualified counsel for any legal issues that concern you, your organization, or questions of compliance

Will Your Compliance Plans/Actions Pass a HIPAA HITECH Audit?

To test your compliance and knowledge now we want to give you a flavor for what information that you, as a Business Associate under HITECH must be prepared to provide in case of a HIPAA audit.

The following is a list of 42 items that HHS officials wanted information on within 10 days of their notice of audit from Piedmont Hospital in 2007.

Once they review your responses and complete the audit then they will decide the penalties due per the chart below:

Violation	Penalty/Violation	Maximum per Year
Tier A - Did not Know	100	25,000
Tier B - Reasonable cause, not willful neglect	$1,000	100,000
Tier C - "Willful Neglect", corrected	$10,000	$250,000
Tier D - "Willful Neglect", uncorrected	$50,000	$1,500,000

In addition to fines your firm could be put under HHS/OCR guidance as CVS has been for up to 20 years requiring much more detailed and regular reporting.

Specifically, Piedmont was asked to provide policies and procedures for:

1. Establishing and terminating users' access to systems housing electronic patient health information (ePHI).
2. Emergency access to electronic information systems.
3. Inactive computer sessions (periods of inactivity).
4. Recording and examining activity in information systems that contain or use ePHI.
5. Risk assessments and analyses of relevant information systems that house or process ePHI data.
6. Employee violations (sanctions).
7. Electronically transmitting ePHI.
8. Preventing, detecting, containing and correcting security violations (incident reports).
9. Regularly reviewing records of information system activity, such as audit logs, access reports and security incident tracking reports.
10. Creating, documenting and reviewing exception reports or logs. Please provide a list of examples of security violation logging and monitoring.
11. Monitoring systems and the network, including a listing of all network perimeter devices, i.e. firewalls and routers.
12. Physical access to electronic information systems and the facility in which they are housed.
13. Establishing security access controls; (what types of security access controls are currently implemented or installed in hospitals' databases that house ePHI data?).
14. Remote access activity i.e. network infrastructure, platform, access servers, authentication, and encryption software.
15. Internet usage.
16. Wireless security (transmission and usage).
17. Firewalls, routers and switches.

Disclaimer: This document and its references do not constitute legal advice. Consult qualified counsel for any legal issues that concern you, your organization, or questions of compliance

18. Maintenance and repairs of hardware, walls, doors, and locks in sensitive areas.
19. Terminating an electronic session and encrypting and decrypting ePHI.
20. Transmitting ePHI.
21. Password and server configurations.
22. Anti-virus software.
23. Network remote access.
24. Computer patch management.
25. Please provide a list of all information systems that house ePHI data, as well as network diagrams, including all hardware and software that are used to collect, store, process or transmit ePHI.
26. Please provide a list of terminated employees.
27. Please provide a list of all new hires.
28. Please provide a list of encryption mechanisms use for ePHI.
29. Please provide a list of authentication methods used to identify users authorized to access ePHI.
30. Please provide a list of outsourced individuals and contractors with access to ePHI data, if applicable. Please include a copy of the contract for these individuals.
31. Please provide a list of transmission methods used to transmit ePHI over an electronic communications network.
32. Please provide organizational charts that include names and titles for the management information system and information system security departments.
33. Please provide entity wide security program plans (e.g System Security Plan).
34. Please provide a list of all users with access to ePHI data. Please identify each user's access rights and privileges.
35. Please provide a list of systems administrators, backup operators and users.
36. Please include a list of antivirus servers, installed, including their versions.
37. Please provide a list of software used to manage and control access to the Internet.
38. Please provide the antivirus software used for desktop and other devices, including their versions.
39. Please provide a list of users with remote access capabilities.
40. Please provide a list of database security requirements and settings.
41. Please provide a list of all Primary Domain Controllers (PDC) and servers (including Unix, Apple, Linux and Windows). Please identify whether these servers are used for processing, maintaining, updating, and sorting ePHI.
42. Please provide a list of authentication approaches used to verify a person has been authorized for specific access privileges to information and information systems.

The Bottom Line

Compliance is NOT a one-time event is a now a core business requirement

All CEs *AND* BAs must meet, and continuously stay in, compliance with all HIPAA and HITECH requirements!

Disclaimer: This document and its references do not constitute legal advice. Consult qualified counsel for any legal issues that concern you, your organization, or questions of compliance

Appendix I - Legal Definitions from the HIPAA Law

Business Associate:

(1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving **the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing**; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, **legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services** to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

(3) **A covered entity may be a business associate of another covered entity**.

Transaction ***means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:***

- Health care claims or equivalent encounter information.
- Health care payment and remittance advice.
- Coordination of benefits.
- ***Health care claim status.***
- ***Enrollment and disenrollment in a health plan.***
- ***Eligibility for a health plan.***
- ***Health plan premium payments.***
- Referral certification and authorization.
- First report of injury.
- ***Health claims attachments.***
- Other transactions that the Secretary may prescribe by regulation.

Trading partner agreement

means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (***For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)***

Disclaimer: This document and its references do not constitute legal advice. Consult qualified counsel for any legal issues that concern you, your organization, or questions of compliance

Health Information

means any information, whether ***oral or recorded in any form or medium***, that:

(1) Is ***created or received by a*** health care provider, health plan, public health authority, ***employer, life insurer***, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; ***or the past, present, or future payment for the provision of health care to an individual***.

Use means, with respect to individually identifiable health information, ***the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information***.

Individually Identifiable Health Information

is information that is a subset of health information, ***including demographic information collected from an individual***, and:

(1) ***Is created or received*** by a health care provider, ***health plan, employer***, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the ***past, present, or future payment for the provision of health care to an individual***; and

(i) That identifies the individual; or

(ii) ***With respect to which there is a reasonable basis to believe the information can be used to identify the individual***.

Protected Health Information

means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) Records described at 20 U.S.C. 1232g (a)(4)(B)(iv); and

(iii) Employment records held by a covered entity in its role as employer.

Disclaimer: This document and its references do not constitute legal advice. Consult qualified counsel for any legal issues that concern you, your organization, or questions of compliance